

REMARKS

IN THE SPECIFICATION

The Office Action objected to the specification as indicated. According to the foregoing, the specification is amended. Withdrawal of the specification objection is respectfully requested.

35 USC 112, SECOND PARAGRAPH, AND 101 REJECTIONS

The Office Action rejected claims 1, 10, 14-15, 17 and 18-31 under 35 USC 112, second paragraph, for being indefinite.

Claims 18-31 are rejected under 35 USC 101 for allegedly being directed to non-statutory subject matter as indicated.

According to the foregoing, the claims are cancelled without disclaimer or prejudice, and the claims are amended taking into consideration the Examiner's comments.

Regarding claim 1 and the language "takes action ~~to execute~~ executing the agreement according to the verification of the conditions ~~of the agreement are satisfied~~," it is submitted that one skilled in the art would understand that an action can be taken depending on whether a condition of an agreement has been verified, such that the claim is not vague. In other words, the scope of the claim is clear to one skilled in the art (see MPEP 2171). Further, the applicant regards as their invention, taking any action depending on agreement verification.

Regarding claim 11, the scope of the language "the trusted secure transaction server supplies a token as confirmation of the payment," is also clear to one skilled in the art as evidenced by the Office Action indicating a token can be provided as payment confirmation to the consumer, the merchant, or both (as the case may be). Further, the applicant regards as their invention the same and the claim is not too broad. For example, paragraph 603 supports claim 11.

Withdrawal of indefiniteness and non-statutory subject matter rejection is requested.

35 USC 103 REJECTIONS

Claims 1-31 are pending.

Claims 1-20, 24, 29 and 31 are rejected under 35 USC 103 for being obvious over Kuroda (US Patent No. 6,470,448) in view of Husemann (US Publication No. 2001/0037264).

Claims 21-23 and 25-26 are rejected under 35 USC 103 for being obvious over Kuroda, Husemann, and Deshpande (US Publication No. 2002/0176579).

Claims 27-28 are rejected under 35 USC 103 for being obvious over Kuroda, Husemann, and Dievondorff (US Patent No. 5,465,328).

In accordance with the foregoing, the specification and claims are amended. Thus, the pending claims remain for reconsideration, which is respectfully requested.

No new matter has been added.

The independent claim is 1, which is rejected over Kuroda and Husemann. According to the foregoing, independent claim 1 is amended by requiring some features of dependent claims 3, 5 and 7. In contrast to Kuroda and Husemann, claim 1 embodiment provides:

1. (CURRENTLY AMENDED) A system for conducting an agreement between two parties relying on a trusted third party comprising:

a mobile device as a first party independently of the second and third party generating a first view of the agreement secured based upon both a first mobile device parameter stored in the mobile device and a second mobile device parameter input to the mobile device and transmitting the first view of the agreement to the ~~third~~second party;

a second party independently of the first and third party generating a second secured view of the agreement and transmitting the second secured view of the agreement to the third party;

an open and non-secure wireless network connecting the first party and the second party,party and transmitting the first view of the agreement from the first party to the second party; and

a wired or wireless network connecting the second party to the third ~~party~~party and transmitting the first and second views of the agreement to the third party,

wherein the trusted third party, receiving the first view of the agreement and the second view of the agreement, verifying verifies conditions of the agreement including that the identities of the first and second parties that transmitted the agreements and that in the independent secured first and second views of the agreement are consistent with each other, based upon a symmetric agreement verification protocol using the first and second mobile device parameters for the secured first view, and takes action to ~~execute~~executing the agreement according to the verification of if the conditions of the agreement are satisfied (emphasis added).

For example, the present Application paragraphs 478+ support the claim amendments. A benefit of the claimed embodiment permits conducting a secured transaction between a consumer mobile device and a merchant over "an open and non-secure wireless network

connecting the first party and the second party, party and transmitting the first view of the agreement from the first party to the second party."

The Office Action in rejecting dependent claim 4 relies upon Kuroda column 13, line 44 to column 14, line 28 for allegedly discussing a "**symmetric agreement verification protocol**." However, Kuroda column 13, line 44 to column 14, line 28 uses an asymmetric security scheme by using a public key and private keys of transaction parties. In contrast, in a symmetric security scheme the parties use one key.

Further, in rejecting dependent claim 5, the Office Action relies upon Kuroda column 2, lines 30-34 for discussing an open and not-secure wireless network. However, Kuroda column 2, lines 30-34 only discuss "safety of a transaction ... between two interested parties is guaranteed by utilizing a communication network," which is silent on whether the communication network is wireless, open and non-secure, or whether a symmetric security scheme is used in an open, non-secure wireless network.

Further, in contrast to Kuroda, the claimed embodiment uses a "**symmetric agreement verification protocol**" in a network configuration in which "**a mobile device... generating a first view of the agreement secured based upon both a first mobile device parameter stored in the mobile device and a second mobile device parameter input to the mobile device**" and "**an open and non-secure wireless network connecting the first party and the second party, party and transmitting the first view of the agreement from the first party to the second party."**

Further, Husemann is only relied upon for discussing a commercial transaction scheme using a mobile device, but fails to disclose either expressly or implicitly any security measures over an open, non-secure wireless network. In particular, Husemann paragraph 100 expressly teaches away from the claimed embodiment by discussing "since the payment process is done via a secure and we established channel between the customer and the carrier, there is no need for encryption of the transaction ..."

Accordingly, a prima facie case of obviousness based upon Kuroda and Husemann has not been established, because a combination of Kuroda and Husemann fails to disclose, either expressly or implicitly, because there is no evidence in either Kuroda or Husemann, or that knowledge of one skilled in the art would motivate modifying Husemann to provide a security scheme other than a secured communication channel, or motivate modifying Kuroda's security scheme to provide the claimed "**symmetric agreement verification protocol**" in a network configuration in which "**a mobile device... generating a first view of the agreement secured based upon both a first mobile device parameter stored in the mobile device and a**

second mobile device parameter input to the mobile device” and “an open and non-secure wireless network connecting the first party and the second party, party and transmitting the first view of the agreement from the first party to the second party.” and seen the benefit of conducting mobile device transactions among a first, second and a trusted third party over an open, non-secure, wireless communication network.

Further, in contrast to Kuroda and Husemann, the claim 8 embodiment provides:

8. (CURRENTLY AMENDED) The system as in claim ~~7~~claim 2 wherein;

the mobile device stores ~~no~~input second mobile device parameter is personal identifying information about the consumer as consumer identifying information and not stored in the consumer mobile device, or account information of the consumer and

~~such account information of the merchant and the consumer is stored in the trusted secure transaction server~~stores or is accessible by the secure transaction server accesses the consumer identifying information.

In rejecting dependent claim 8, the Office Action only relies on Kuroda FIG. 1 and alleges because the user's terminal devices do not have a storage unit, therefore they are not storing any data. However, Kuroda is silent on whether the user terminals store any user identifying information, and further Kuroda would store the private key of the user to generate a digital signature.

Dependent claims recite patentably distinguishing features of their own or are at least patentably distinguishing due to their dependencies from the independent claim 1.

In view of the claim amendments and remarks, withdrawal of the rejection of the claims and allowance of claims is respectfully requested.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,
STAAS & HALSEY LLP

Date: June 8, 2007

By: / Mehdi D. Sheikerz /
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501